Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 70 (2015) 808 – 813

Procedia Computer Science

4th International Conference on Eco-friendly Computing and Communication Systems

Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks

Monika[a*], Shuchita Upadhyaya[a]

[a]*Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, 136118, Haryana, India*

Abstract

Security is one of the most significant and fundamental issue for data transmission in WSNs. DNA cryptography plays a very vital role in the areas of communications and data transmission. In DNA cryptography, biological DNA concept can be used not only to store data and information carrier, but also to perform computations. This paper is based on computation security using DNA cryptography. An algorithm is proposed that uses DNA cryptography with secure socket layer (SSL) for providing a secure channel with more secure exchange of information in wireless sensor networks.

Peer-review under responsibility of the Organizing Committee of ICECCS 2015

Keywords: DNA cryptography; Secure Socket Layer (SSL); Wireless sensor networks; Encryption; Decryption.

1. Introduction

Wireless sensor networks (WSNs) comprise an enormous number of small sensor nodes that send the collected information using the wireless channels. This sensor network is a heterogeneous system combining tiny sensors and actuators with computing elements. Most sensor networks consist of thousands of low power, less- cost nodes

* Corresponding author. Tel.: +91-9896597808
E-mail address: monikaporiye@gmail.com

Peer-review under responsibility of the Organizing Committee of ICECCS 2015
doi:10.1016/j.procs.2015.10.121

deployed to monitor and affect the environment. WSNs have many applications such as traffic control, health monitoring and environment monitoring etc[1, 2]. Most of the applications of WSNs require secure transmission of information at both ends. Therefore security in WSNs is a critical issue because sensor nodes have limited storage and energy for processing. When these sensor nodes are deployed in any environment, the problem of secured sharing of keys between sensor nodes becomes an issue of consideration as sensor nodes are prone to various types of undesirable attacks [3, 4]. To ensure security, encryption & authentication are the traditional approaches for transmission of data. The main issue here is how to transmit the data securely & to make the organization of secret keys for securing data among the communicating sensor nodes. The secure socket layer (SSL) in wireless sensor networks resolves the problem of sharing of keys between tiny sensor nodes. Among the three basic schemes for key sharing, one is trusted server which anticipate the key agreement between sensor nodes e.g., Kerberos[5]. This scheme may not be suitable for sensor networks because there is usually no trusted infrastructure in these networks. In the second scheme, a key agreement is done using public key cryptography. This scheme may again have its limitations in sensor networks, because of computation overhead leading to more energy consumption which is undesirable in sensor networks. Also it is undesirable to use public key algorithms such as Diffie-Hellman key agreement [6, 7] due to man-in-the-middle attack as pointed out in [8]. In the third type, the keys information is distributed among all sensor nodes before deploying in any environment [9]. The theme of the proposed strategy in this paper utilizes this concept of key distribution to ensure security at the first level where key exchange amongst the nodes has to be done. This paper proposes an enhancement to the key exchange methodology described in[5 - 7].

Cryptography is an art of concealing the data and secures that data or information from various types of attacks. It is a technique of achieving the security by converting the original information or message into coded or unreadable form which is not interpreted by the third party[10]. The evolution of cryptography is attached to human intelligence and evaluation capacities. Biological computing (e.g. DNA computing) and traditional computing are two significant technologies that have been explored in literature. Recent researches have shown that DNA based cryptography is an attractive field which shows strong parallelism and incredible information density. DNA computing utilizes DNA base pairs for communication mode[11].

In the light of above, a need to have a technology which is completely secure or having more protection than existing techniques is realized. In this paper, a technique is proposed in which DNA cryptography with secure socket layer (SSL) are used for providing more secure channel with more secure exchange of information during communication and data transmission.

2. DNA & DNA Cryptography

Deoxyribonucleic acid (DNA) is hereditary material for all living beings and carries the genetic information. DNA consists of two antiparallel biopolymer strands coiled around each other to form a double helix form. DNA is a prolong polymer of compact units called nucleotides. Each DNA strand is composed of four nucleobases: A (Adenine), G (Guanine), C (Cytosine) & T (Thymine) [12]. The detail of any living thing is stored in DNA bases as shown in Fig.1[13].

In DNA cryptography, DNA base pairs are used as the information carrier. Big processing power of DNA chips make it more advanced technique as compared to other techniques which are being used. As a result of this, DNA chips bring forward a new hope for superseding to the current silicon chips in future, which may enhance computer data processing in an enormous fashion. As many traditional cryptographic algorithms (like DES, RSA etc.) have already been broken by many attackers, so need of more secure cryptographic techniques has emerged. DNA computing algorithms have already been proposed for cryptography issues [14-16]. Many algorithms based on DNA cryptography have been designed which use symmetric & asymmetric keys for hiding the data [17-19]. The main advantage of DNA cryptography is extraordinary storage capacity of DNA, low power consumption for computing and high processing time with remarkable performance.

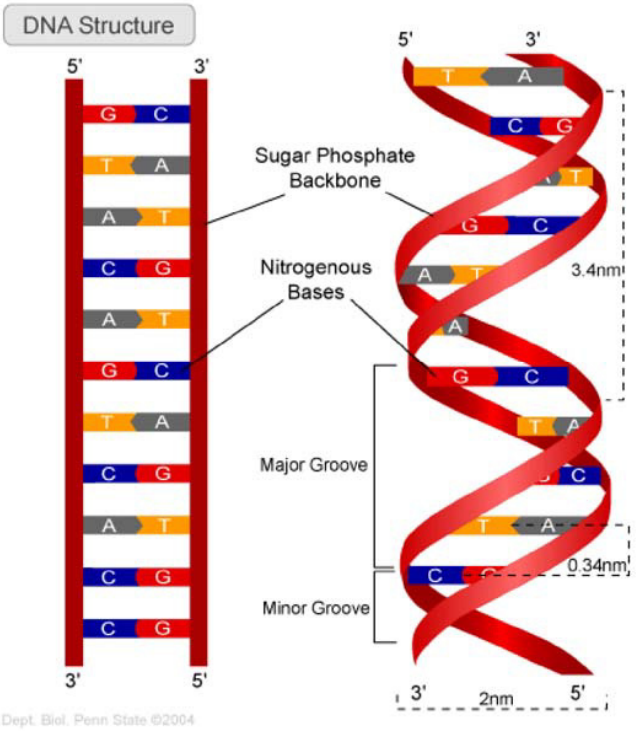

Fig. 1 DNA Structure[13]

3. SSL [20, 21]

SSL is well-known Internet protocol which acts as a secure channel between two nodes. Since 1994, SSL has become the world's most popular security protocol. SSL is having three versions: 2, 3 & 3.1. The most popular is version 3. SSL is basically used to exchange public keys & digital signature between two nodes in a secure manner. Thus both confidentiality & authentication services are offered by SSL. The general concept of SSL is shown in fig. 2.

Fig. 2. SSL Architecture

4. Proposed work

For providing the security in WSN, the key pairs (i.e. public & private key) are used in the proposed algorithm. For the generation of key pairs (encryption/decryption), RSA algorithm is used. As in WSN, the sensor nodes have tiny storage & low power, so key pairs & digital certificate are assigned to the sensor nodes initially before deploying them in any environment. After deploying sensor nodes, each sensor node has a public & private key pair & digital certificate itself. The exchange of public key and digital certificate between sensor nodes is done through

the secure channel (SSL) during communication process. In the proposed system security is achieved in three steps i.e. information, computation and biological.

The encryption process is shown in Fig. 3

Encryption:

Step-1. The exchange of public key is done between two sensor nodes by using the secure socket layer protocol. Thus sensor nodes which want to communicate have public key of each other in a secure manner.

Step-2. Now the original data is secured by applying computation security in the following steps:

1) The plain text is converted into their ASCII values.
2) These ASCII values are encrypted with the public key of another party that wants to communicate.
3) The resulting data values are divided into groups of three digits.
4) These combination of three digits strings are changed to base -4 conversions which yields the data in the form of 0, 1, 2 &3.
5) The above values are converted into binary form.

Step-3. In the last step by using the concept of biological DNA, binary values are changed into their DNA base equivalent like A,C,T & G (as per Table 1) and the data will be transmitted as a sequence of nucleotides.

Table 1. Nucleotide Bases

Nucleotide	Binary Form
A	00
C	01
G	10
T	11

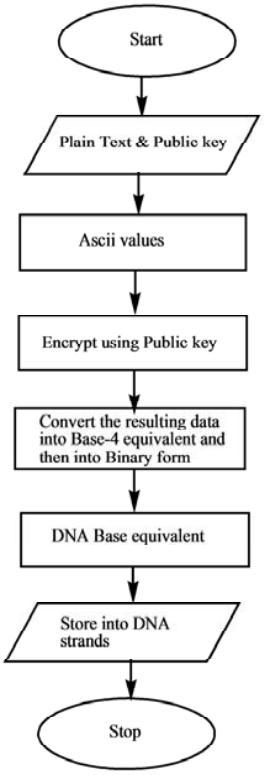

Fig. 3. Encryption Process

5. Decryption

Decryption process is just reverse of the encryption process. Instead of encryption key recipient's private key is used as a decryption key in step 2 of the above process.

6. Comparison of propose DNA cryptography with SSL and other DNA cryptographic techniques

DNA cryptography with SSL may be a better technique than other DNA techniques used for security in the sense that here, security is achieved in three steps. In the first step exchange of public key of sensor nodes is done by using the secure socket layer protocol (key information secure). Thus the problem of energy consumption by sensor nodes for generating key pairs and digital certificate (for authentication) has been resolved because distributed of this information among sensor nodes is done before deploying them in any environment. In the second step encryption is performed with recipient's public key and finally in third step, with the use of the biological DNA concept, binary data is converted into DNA base equivalent. On the other hand previous techniques[14-16] based on DNA cryptography provided security in two steps (computation as well as biological). Moreover in the proposed work seven security principles are achieved i.e. Authentication, integrity, confidentiality, Non-repudiation, Access control, availability & signature. Whereas in previous DNA cryptographic techniques only four security principles (Authentication, integrity, confidentiality & Non-repudiation) were achieved.

7. Conclusion

DNA cryptography is concealing the data in terms of DNA bases. This is done by using many DNA techniques. Here in this paper, the DNA concept for encryption with SSL protocol is used, which gives us three levels of security in WSN. In our proposed system the energy consumption problem for generating key pairs & generating certificates for sensor nodes are resolved to some extent by assigning key pairs & digital certificate before deploying sensor nodes in any environment. The public key & digital certificate sharing is done using the secure channel (SSL). Thus the computation overhead for sensor nodes for generating the keys may be reduced which may in turn reduce the computation time leading to energy efficiency in sensor nodes. It is anticipated that the solution proposed may provide promising results. An implementation of the algorithm is under process for both encryption and decryption.

References

1. Yick J, Mukherjee B, Ghosal D. Wireless sensor network survey. *Computer Networks*, 2008; 52 (12): 2292-2330.
2. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. *Communications Magazine, IEEE* 2002; 40: 102–114.
3. Chen X, Makki K, Yen K, Pissinou N. Sensor Network Security: *A Survey. IEEE Communications Surveys & Tutorials* 2009; 11 (2): 52-73.
4. Patel MM, Aggarwal A. Security attacks in wireless sensor networks: A survey. *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on* 2013. p. 329–333.
5. Neuman BC, Tso T. Kerberos: an authentication service for computer networks. *Communications Magazine, IEEE* 1994; 32(9): 33–38.
6. Diffie W, Hellman ME. New directions in cryptography. *Information Theory, IEEE Transactions on* 1976; 22: 644–654.
7. Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 1978; 21(2): 120–126.
8. Perrig A, Szewczyk R, Wen V, Cullar D, Tygar JD. Spins: Security protocols for sensor networks. *Proceedings of the 7th annual international conference on Mobile computing and networking* 2001. p. 189–199.
9. Du W, Deng J, Han YS, Chen S, Varshney PK. A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies* 2004. p. 597.
10. Kahate A. *Cryptography Techniques. Cryptography and Network Security.* 3rd ed. New Delhi,India: McGraw; 2014; p. 32-36.
11. Pramanik S, Setua SK. DNA Cryptography. *7th International Conference on Electrical and Computer Engineering* 2012. p. 551 – 554.
12. en.wikipedia.org/wiki/DNA
13. DNA-Structure, https://sites.google.com/site/imlovingmygenes.
14. Mandge T, Choudhary V. A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme. *Information Communication and Embedded Systems (ICICES), 2013 International Conference on* 2013. p. 47-52.
15. Sadeg S, Gougache M, Mansouri N, Drias H. An encryption algorithm inspired from DNA. *Machine and Web Intelligence (ICMWI), 2010 International Conference on* 2010. p. 344 - 349.
16. Guozhen X, Mingxin L, Lei Q, Xuejia L. New field of cryptography: DNA cryptography. *Chin. Sci. Bull.* 2006; 51 (12): 1413-1420.

17. Zhang Y, Xiao D, Wen W, Wong KW. On the security of symmetric ciphers based on DNA coding. *Information Sciences* 2014; 289: 254–261.
18. Cui G, Qin L, Wang Y, Zhang X. An Encryption Scheme Using DNA Technology. *Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008. 3rd International Conference on* 2008. p. 37-42.
19. Tripathi SPN, Jaiswal M, Singh V. Securing DNA Information through Public Key Cryptography. *MIS Review* 2013; 19 (1): 45-59.
20. Panwar MPK, Kumar MD. Security through SSL. *International Journal of Advanced Research in Computer Science and Software Engineering* 2012; 2(12): 178-184.
21. Lee HK, Malkin T, Nahum E. Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices. *IMC '07 Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* 2007. p. 83-92.